CLAIMS

1.   An information processing apparatus comprising:

means for storing content data;

a controlling means having a software which controls storage or read of the content data into or from the content data storage means; and

means provided in a hardware independent of the controlling means to decrypt and execute an encrypted program supplied from the controlling means and supply the result of the program execution to the controlling means;

the controlling means controlling the content data storage or read to or from the content data storage means based on the program execution result supplied from the program executing means.

2.   The apparatus as set forth in Claim 1, wherein:

the content data storage means stores also management information with which the content data stored in itself is managed; and

the controlling means makes the program executing means execute a predetermined computation based on the management information.

3.   The apparatus as set forth in Claim 1, wherein:

the controlling means is a CPU;

the content data storing means is a hard disc; and

the program executing means is a CPU incorporated in a semiconductor IC

other than a one in which the CPU as the controlling means is built.

4.   (Amended)   An information processing apparatus comprising:

a storage medium for storing content data and content management information for the content data;

a process controller formed from a software to control storage or read of content data into or from the storage medium; and

a program execution controller provided in a semiconductor chip independent of the process controller and which is supplied with an encrypted program from the process controller, decrypts the program and supplies the result of the program execution to the process controller;

the process controller controlling storage or read of the content data into or from the storage medium based on the result of the program execution by the program execution controller; and

the program execution controller being adapted so that its internal operations cannot be confirmed from outside the semiconductor chip, and making a computation for checking any falsification made to the content management information.

5.   (Amended)   An information processing method for use in an information processing apparatus comprising:

means for storing content data;

a controlling means having a software which controls storage or read of the content data into or from the content data storage means; and

means provided in a hardware independent of the controlling means to decrypt and execute an encrypted program supplied from the controlling means and supply the result of the program execution to the controlling means;

the method comprising a step of:

controlling storage or read of content data into or from the content data storage means based on the result of the program execution by a program executing means.

6.   (Amended)   An information processing method for use in an information processing apparatus comprising:

a storage medium for storing content data and content management information for the content data;

a process controller formed from a software to control storage or read of content data into or from the storage medium; and

a program execution controller provided in a semiconductor chip independent of the process controller and which is supplied with an encrypted program from the process controller, decrypts the program and supplies the result of the program execution to the process controller;

the process controller controlling storage or read of the content data into or from the storage medium based on the result of the program execution by the program execution controller; and

the program execution controller being adapted so that its internal operations cannot be confirmed from outside the semiconductor chip, and making a computation

for checking any falsification made to the content management information.

7.   (Amended)   A program storage medium for use in an information processing apparatus comprising:

means for storing content data;

a controlling means having a software which controls storage or read of the content data into or from the content data storage means; and

means provided in a hardware independent of the controlling means to decrypt and execute an encrypted program supplied from the controlling means and supply the result of the program execution to the controlling means;

the controlling means having recorded therein a computer-readable program comprising a step of controlling storage or read of the content data into or from the content data storing means based on the result of the program execution by the program executing means.

8.   (Amended)   An information processing apparatus comprising:

means for inputting content data;

means for storing the content data supplied from the input means;

means for compressing the content data stored in the content data storing means in a predetermined manner;

means for encrypting the data stored in the content data storing means in a predetermined manner; and

means for controlling storage or read, into or from the content data storing

means, of the content data compressed by the compressing means and encrypted by the encrypted means.

9.   (Amended)   The apparatus as set forth in Claim 8, wherein the compressing means compresses, or the encrypting means encrypts, different data supplied from the input means in the same manner.

10.   (Amended) The apparatus as set forth in Claim 8, wherein the compressing means compresses, or encrypting means encrypts, different data supplied from the input means in different manners, respectively, and takes a predetermined common compressing or encrypting manner for outputting the data read from the content data storing means to a predetermined apparatus.

11.   (Amended) An information processing apparatus comprising:

an interface via which content data is supplied from a predetermined recording medium or server;

a storage medium for storing content data supplied via the interface;

a compression program for compressing content data for storage into the storage medium in a predetermined manner;

an encryption program for encrypting the content data for storage into the storage medium in a predetermined manner; and

a controller for controlling storage or read, into or from the storage medium, the content data having been compressed by the compression program and encrypted by the encryption program;

the compression program compressing, or the encryption program encrypting, content data supplied via the interface and having been processed in different manners, in the same manner or different manners, respectively, for storage into the storage medium, and converting, when reading from the storage medium the content data having been compressed or encrypted in the different manners, respectively, for delivery to a predetermined portable device, the content data so that they can be compressed or encrypted in a common manner to both this apparatus and portable device.

12. (Amended) An information processing method comprising the steps of:

inputting data;

storing the data supplied from the data input step;

compressing the data stored at the data storing step in a predetermined manner;

encrypting the data stored at the data storing step in a predetermined manner; and

controlling storage or read of the data compressed at the compressing step and encrypted at the encrypting step.

13. (Amended) An information processing method comprising the steps of:

inputting content data from a predetermined recording medium or server;

storing content data supplied at the data input step;

compressing the content data stored at the data storing step in a predetermined manner;

encrypting the content data stored at the compressing step in a predetermined manner; and

controlling storage or read, into or from the storage medium, the content data having been compressed at the compressing step and encrypted at the encrypting step;

the compressing step compressing, or the encryption step encrypting, content data supplied at the data input step and having been processed in different manners, in the same manner or different manners, respectively, for storage into the storage medium, and converting, when reading from the storage medium the content data having been compressed or encrypted in the different manners, respectively, for delivery to a predetermined portable device, the content data so that they can be compressed or encrypted in a common manner to both this apparatus and portable device.

14.   (Amended)   A program storage medium having recorded therein a program intended for execution by an information processing apparatus and readable by a computer, the program comprising the steps of:

inputting data;

storing the data supplied from the data input step;

compressing the data stored at the data storing step in a predetermined manner;

encrypting the data stored at the data storing step in a predetermined manner; and

controlling storage or read of the data compressed at the compressing step and

encrypted at the encrypting step.

15. (Amended) An information processing apparatus comprising:

means for inputting content data;

means for storing the content data supplied from the content data input means;

means for holding management information for the content data stored in the content data storing means;

means for making a predetermined computation based on the management information held in the management information holding means; and

means for controlling the usage of the content data stored in the content data storing means according to a result of a comparison made between the result of the computation made by the computing means and that of the past computation which is stored in the content data storing means.

16. (Amended) The apparatus as set forth in Claim 15, wherein the computing means makes the computation using a hash function as the management information.

17. (Amended) The apparatus as set forth in Claim 15, wherein the data is music data and the management information includes identification information for identification of the music data.

18. (Amended) An information processing apparatus comprising:

an interface for input of content data and identification information of the content data;

a storage medium for storing content data supplied via the interface;

a first memory for holding, as a usage rule file, the identification information of the content data stored in the storage medium;

a management program for making a computation with the hash function applied to the identification information held in the first memory;

a second memory for storing the result of the computation by the management program; and

a controller for comparing the result of the computation by the management program with the past computation result stored in the second memory to inhibit, when there is no coincidence between the computation results, copy or move of the content data stored in the storage medium.

19.   (Amended)   An information processing method comprising the steps of:

inputting data;

storing the data supplied at the data input step;

holding management information for the data stored at the data storing step;

making a predetermined computation based on the management information held at the management information holding step;

storing the result of the computation made at the computing step; and

comparing the result of the computation made at the computing step with a past computation result stored at the data storing step to control the usage of the data stored at the data storing step.

20.   (Amended)   An information processing method comprising steps of:

inputting content data and identification information of the content data;

storing the content data supplied at the input step into a storage medium;

holding, as a usage rule file, the identification information of the content data stored at the storing step;

making a computation with the hash function applied to the identification information held at the holding step;

storing the result of the computation made at the computing step; and

comparing the result of the computation at the computing step with a past computation result stored at the storing step to inhibit, when there is no coincidence between the computation results, copy or move of the content data stored in the storage medium.

21.   (Amended)   A program storage medium having recorded therein a program intended for execution by an information processing apparatus and readable by a computer, the program comprising the steps of:

inputting data;

storing the data supplied from the data input step;

holding management information for the data stored at the data storing step;

making a predetermined computation based on the management information held at the management information holding step;

storing the result of the computation made at the computing step; and

controlling the usage of the data stored at the data storing step according to a

result of a comparison made between the result of the computation made at the computing step and that of the past computation stored at the data storing step.

22.   (Amended)   An information processing apparatus comprising:

means for transmitting and receiving data to and from other apparatus;

means for holding a predetermined lock key and save key;

authenticating means which uses the lock key held in the holding means when transmitting and receiving data to and from the other apparatus to make a mutual authentication with the other apparatus to generate a communication key;

means for encrypting the communication key with the save key; and

means for storing the data received by the data transmitting and receiving means and having been encrypted with the communication key correspondingly to the communication key encrypted by the encrypting means.

23.   (Amended)   The apparatus as set forth in Claim 22, further comprising:

an encryption key decrypting means for decrypting the communication key stored in the storing means using the save key; and

means for decrypting the data stored in the storing means.

24.   (Added)   An information processing apparatus comprising:

an interface via which data is transferred between the apparatus and a portable device or server connected to the apparatus;

a memory for holding predetermined master key and save key;

an authentication program which uses, when the data is to be transferred to or

from the portable device or server, the master key stored in the memory to make a mutual authentication with the portable device or server to generate a communication key;

an encryption decryption program to decrypt, with the communication key, an encryption key with which the content data transmitted from the portable device or server has been encrypted and encrypt the encryption key with the save key;

a storage medium for storing the content data received via the interface and encrypted with the communication key in correspondence with the encryption key encrypted with the save key;

an encryption key decryption program to decrypt, with the save key, the encryption key stored in the storage medium; and

a data decryption program to decrypt content data stored in the storage medium with the encryption key decrypted by the encryption decryption program.

25.   (Added) An information processing method comprising the steps of:

transmitting and receiving data to and from other apparatus;

holding a predetermined lock key and save key;

using the lock key held at the holding step when transmitting and receiving data to and from the other apparatus to make a mutual authentication with the other apparatus to generate a communication key;

encrypting the communication key with the save key; and

storing the data received at the data transmitting and receiving step and having

been encrypted with the communication key correspondingly to the communication key encrypted at the encrypting step.

26.   (Added)   An information processing method comprising the steps of:

transferring data between the apparatus and a portable device or server connected to the apparatus;

holding predetermined master key and save key;

mutually authenticating with the portable device or server, when data is to be transferred to or from the portable device or server, using the master key held at the holding step to generate a communication key;

decrypting, with the communication key, an encryption key with which the content data transmitted from the portable device or server has been encrypted and encrypting the encryption key with the save key;

storing the content data received via the interface and encrypted with the communication key in correspondence with the encryption key encrypted with the save key;

decrypting, with the save key, the encryption key stored in the storage medium at the storing step; and

decrypting content data stored in the storage medium with the encryption key decrypted at the encryption decrypting step.

27.   (Added)   A program storage medium having recorded therein a program intended for execution by an information processing apparatus and readable by a

computer, the program comprising the steps of:

transmitting and receiving data to and from other apparatus;

holding a predetermined lock key and save key;

using the lock key held at the holding step when transmitting and receiving data to and from the other apparatus to make a mutual authentication with the other apparatus to generate a communication key;

encrypting the communication key with the save key; and

storing the data received at the data transmitting and receiving step and having been encrypted with the communication key correspondingly to the communication key encrypted at the encrypting step.

28. (Added)   An information processing apparatus comprising:

means for storing data;

means for holding the usage rule for the data stored in the data storing means;

means for judging whether or not, when moving the data stored in the data storing means to other apparatus, the usage rule for the data stored in the data storing means is reproducible by the other apparatus; and

means for moving, based on the result of the judgment by the judging means, the data stored in the data storing means to the other apparatus along with the usage rule for the data stored in the data storing means, which is held in the holding means.

29. (Added)   The apparatus as set forth in Claim 28, wherein the usage rule for the data include:

playback limiting condition;

playback accounting condition; or

copy limiting condition.

30. (Added) An information processing apparatus comprising:

a storage device to store contend data;

a memory to hold a usage rule for the content data stored in the storage device; and

a move management program to judge, when the content data stored in the storage device is to be moved to a portable device, whether the portable device meets the usage rule;

move of the content data stored in the storage device to the portable device being inhibited when it is determined as the result of the judgment by the move management program that the portable device does not meet the usage rule.

31. (Added) The apparatus as set forth in Claim 30, wherein the move includes copy, move or check-out, and the usage rule includes playback limiting condition, playback accounting condition or copy limiting condition.

32. (Added) An information processing method comprising steps of:

storing data;

holding the usage rule for the data stored at the data storing step;

judging whether or not, when moving the data stored at the data storing step to other apparatus, the usage rule for the data stored at the data storing step is

reproducible by the other apparatus; and

moving, based on the result of the judgment at the judging step, the data stored in the data storing means to the other apparatus along with the usage rule for the data stored at the data storing step, which is held at the holding step.

33.   (Added)   An information processing method comprising steps of:

storing contend data into a storage device;

holding in a memory a usage rule for the content data stored in the storage device; and

judging, when the content data stored in the storage device is to be moved to a portable device, whether the portable device meets the usage rule;

inhibiting move of the content data stored in the storage device to the portable device when it is determined that the portable device does not meet the usage rule.

34.   (Added) The method as set forth in Claim 33, wherein the move includes copy, move or check-out, and the usage rule includes playback limiting condition, playback accounting condition or copy limiting condition.

35.   (Added)   A program storage medium having recorded therein a program intended for execution by an information processing apparatus and readable by a computer, the program comprising steps of:

storing data;

holding the usage rule for the data stored at the data storing step;

judging whether or not, when moving the data stored at the data storing step to

other apparatus, the usage rule for the data stored at the data storing step is reproducible by the other apparatus; and

moving, based on the result of the judgment at the judging step, the data stored in the data storing means to the other apparatus along with the usage rule for the data stored at the data storing step, which is held at the holding step.